

## ABSTRACT

A fast encryption method particularly useful for long message lengths is provided. A message  $m$  is encrypted using a transmitter secret key  $z$  to form a quantity  $E$ . A transmitter processor prepares a quadruplet  $(a_{\text{new}}, b_{\text{new}}, s_{\text{new}}, E)$  where:

$$\begin{aligned} a_{\text{new}} &= z * y^c \text{ modulo } p ; \\ b_{\text{new}} &= g^c \text{ modulo } p ; \\ s_{\text{new}} &= \text{signature}_c(a_{\text{new}}, b_{\text{new}}, E). \end{aligned}$$

As in previous embodiments  $y = g^x \text{ modulo } p$  is the public key and  $x$  is the receiver secret key. The parameters  $g$ ,  $x$ , and  $p$  according to methods known to a person skilled in the art and the parameter  $g$  is a generator of the group  $G_p$ . The parameter  $c$  is a random number. The transmitter processor sends the quadruplet  $(a_{\text{new}}, b_{\text{new}}, s_{\text{new}}, E)$  to a receiver processor. The receiver processor verifies the signature on  $s_{\text{new}}$  using methods known in the art. The receiver processor then decrypts  $a_{\text{new}}$  and  $b_{\text{new}}$  using the receiver secret key  $x$  to get the transmitter secret key  $z$ , i.e. in the following manner.  $z = a_{\text{new}}/b_{\text{new}}^x$ . The receiver processor uses the transmitter secret key  $z$  to decrypt  $E$  to get the message  $M$ .